REMARKS

Claims 1-17 are now pending in the application. Applicant amends claims 1, 3, 5, 7 and 15-17 and cancels claims 2, 4, 6 and 9 herein. The Examiner is respectfully requested to reconsider and withdraw the rejections in view of the amendments and remarks contained herein.

REJECTION UNDER 35 U.S.C. § 101

Claims 16 and 17 stand rejected under 35 U.S.C. § 101 as being directed to "A network security enhancing program", which is merely an example of functional descriptive material and is nonstatutory under 35 U.S.C. § 101. Claims 16 and 17 are amended to recite a “program product being stored on a computer-readable medium”. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

REJECTION UNDER 35 U.S.C. § 112

Claims 7 and 15 stand rejected under 35 U.S.C. § 112, first paragraph. This rejection is respectfully traversed. Notwithstanding and in the interest of expediting prosecution, Applicant amends claims 7 and 15 to address the issue raised by the Examiner. Since claims 7 and 15 are no longer directed to a single means, reconsideration and withdrawal of this rejection are respectfully requested.

CLAIM OBJECTIONS

Claim 9 stands objected to as containing informalities. Claim 9 is cancelled. Accordingly, this rejection is moot.

REJECTION UNDER 35 U.S.C. § 102

Claims 1, 2, 4-6, 15 and 17 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Burns (U.S. Pat. Pub. No. 2004/0103317). Claims 1-17 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Albert et al. (U.S. Pat. Pub. No. 2003/0177389) – including the reference incorporated by reference Freund et al. (U.S. Pat. Pub. No. 2003/0055962). These rejections are respectfully traversed. Notwithstanding, Applicant amends claims 1, 3, 5, 7, 15, 16 and 17, and cancels claims 2, 4, 6 and 9. Please note that the amendments made herein assume that the Article 34 amendments were not entered. Of the above noted amended claims, claims 1, 5, 7, 15, 16 and 17 are independent.

Amended claim 1 calls for a method in which a computer acquires particular data through a network. The method includes: detecting a first activation instruction to activate a program that connects to the network and sends and receives communications in a state that the already-operating computer is not connected to the network; performing particular data acquisition processing for acquiring the particular data through the network, when a first activation instruction to activate the program is detected; and thereafter, activating the program whose activation has been instructed.

Amended claim 5 calls for a system for acquiring particular data through a network including: a means that detects a first activation instruction to activate a program that connects to the network and sends and receives communications, in a state that the already-operating computer is not connected to the network; a means that performs particular data acquisition processing for acquiring particular data through the

network, when a first activation instruction to activate the program is detected; and a means that activates the particular program whose activation has been instructed, after the particular data acquisition processing.

Amended claim 7 calls for a network security enhancing system for a computer, comprising: a means that detects a first activation of a program that connects to a network and sends and receives communications in a state that the already-operating computer is not connected to the network; and a means that activates processing of updating a security file at activation of the program, after processing of connection to the network and before other processing.

Amended claim 15 calls for a network security enhancing system for computer, wherein: a means that detects a program that is installed on the computer and connects to a network and sends and receives communications, a means that detects an activation instruction of a program that connects to the network and sends and receives communications, a means that activates network connection processing, a means that detects first activation of a program that connects to the network and sends and receives communications, in a state that an already-operating computer is not connected to the network, a means that activates the processing of updating the security file at activation of the program, after processing of connection to the network and before other processing.

Amended claim 16 calls for a network security enhancing program product being stored on a computer-readable storage medium, wherein: the network security enhancing program makes a computer operate: to detect first activation of a program that communicates to a network in a state that the already-operating computer is not

connected to the network; and to activate processing of updating a security file at activation of the program, after connection to the network and before other processing.

Amended claim 17 calls for a network security enhancing program product being stored on a computer-readable storage medium, wherein: the network security enhancing program makes a computer perform which detects a program that has been installed in the computer and connects to the network and sends and receives communication, the processing detects an activation instruction of a program that connects to the network and sends and receives communications, the processing activates processing of connection to the network, the processing detects first activation of a program that connects to the network and sends and receives communications, in a state that an already-operating computer is not connected to the network, the processing activates processing of updating a security file at activation of a program that connects to a network and sends and receives communications, after processing of connection to the network and before other processing, and thereafter activates the program.

For anticipation to be present under 35 U.S.C §102(b), there must be no difference between the claimed invention and the reference disclosure as viewed by one skilled in the field of the invention. *Scripps Clinic & Res. Found. V. Genentech, Inc.*, 18 USPQ.2d 1001 (Fed. Cir. 1991). All of the limitations of the claim must be inherent or expressly disclosed and must be arranged as in the claim. *Constant v. Advanced Micro-Devices, Inc.*, 7 USPQ.2d 1057 (Fed. Cir. 1988). Here, Burns and Albert (including Freund) all fail to disclose the limitation of detecting first activation of a program that connects to a network and sends and receives communications, in a state

that an already-operating computer is not connected to the network as claims 1, 5, 7, 15, 16 and 17 recite.

That is, each of independent claims 1, 5, 7, 15, 16 and 17 recite detecting first activation of a program that connects to a network and sends and receives communications, in a state that an already-operating computer is not connected to the network. The "first activation of a program" advantageously serves to prevent downloading of virus files from a network at each time a communication program is activated after the computer is connected to a network. Neither Burns nor Albert (including Freund) disclose this point, nor recognize the existence of such a problem. Moreover, the claimed invention recognizes a problem which might cause problems of activating a computer. The computer is usable as a normal computing device if any communication program is intervened. In this regard, the present invention is different from Burns and Albert (including Freund).

More particularly, Burns (Burns: Para [0026] Line 12-18 and Para [0016] Line 1-3) explains that a module within a computer intercepts an authentication request and performs the role of interpreting and assessing the security policy stored on the trusted computing device. Further, the above process is performed before the user is allowed to enter their passcode to unlock the trusted computing device. However, neither Burns nor Albert (including Freund) explain the feature of the claimed invention wherein "first activation of a program that sends and receives communications" is detected.

According to Albert (including Freund), in response to receipt of a request from a device for connection to a particular network, a current security policy is applied to the device. Further, Albert (including Freund) discloses that only after the current security

policy is generated or updated, and the updated security policy is applied to the device, the connection to a particular network is allowed. Albert (including Freund) does not disclose or suggest detecting first activation of a program that connects to the network and sends and receives communications as claimed. Moreover, Albert (including Freund) does not mention the desirability of such detection.

Inasmuch as neither Burns nor Albert (including Freund) teach or suggest all of the claim limitations, neither Burns nor Albert (including Freund) can anticipate claims 1, 5, 7, 15, 16 and 17. Therefore, Applicant respectfully requests reconsideration and withdrawal of this rejection.

Dependent claims 3, 8 and 10-14 should be in condition for allowance for at least the same reasons as set forth above with respect to their base claims.

CONCLUSION

It is believed that all of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider and withdraw all presently outstanding rejections. It is believed that a full and complete response has been made to the outstanding Office Action and the present application is in condition for allowance. Thus, prompt and favorable consideration of this amendment is respectfully requested. If the Examiner

Examiner is invited to telephone the undersigned at (248) 641-1600.

Respectfully submitted,

Dated: January 19, 2009

By: /G. Gregory Schivley/
G. Gregory Schivley
Reg. No. 27,382
Bryant E. Wade
Reg. No. 40,344

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 828
Bloomfield Hills, Michigan 48303
(248) 641-1600

[GGS/BEW/pvd]